Digital Security
Progress. Protected.

CYBER**RESILIENCE**  PROTECT

Achieving cyber resilience: ESET's four-step approach to business continuity.

Step 2: Protect

Solid cybersecurity tools, processes and practices are a foundational piece of a cyber-resilience strategy. Well-implemented, multilayered security blocks all manner of threats to greatly reduce the chances of an event that could disrupt the business.

Ransomware gangs, in particular, are resourceful, patient and persistent. If there's a weak link anywhere in your security, they'll find it.

Protecting your organization entails multiple layers of protection, including:

Endpoint protection software on all desktops, laptops, servers and mobile devices that access your network is a must. Look for a system that can be centrally administered, and updates automatically.

Multi-factor authentication effectively protects against compromised passwords that might be used to access your systems.

Encryption makes your data readable to you, but unreadable to an intruder who doesn't have the key. Ransomware attacks typically include an attempt to exfiltrate business-sensitive data and threaten to leak it publicly in an extortion ploy. An intruder who finds encrypted data may look for easier prey, while one who is determined will need to jump through extra hoops to make your information exportable.

Cybersecurity awareness training is a key element. Don't overlook the importance of having security-savvy employees who can recognize phishing attacks, falsified web sites and other suspicious activity. Employees are often the weakest link in your security, but comprehensive cybersecurity training can make them one of the strongest.

ESET Solutions

- **ESET Endpoint Security**
- **ESET Secure Authentication**
- **ESET Endpoint Encryption**
- **ESET Cybersecurity Awareness Training**

Checklist: Mounting a foundational, multilayered defense

- Audit user access—limit access to services, software and data so that only those who need access have it.
- Close ports and stop services that are not used—they provide open doors that can easily be closed.
- Ensure that all endpoints, including servers and mobile devices, are protected with an anti-malware product that is updated and fully operational.
- Look for endpoint security software that goes beyond signature-based detection, and if the advanced features are presented as options, enable them.
- Encourage employees who work remotely to have multi-layered security on their home devices.
- Enforce a policy of strong, secure passwords—or, better yet, strong passphrases.
- Implement two-factor authentication on all external access and for all accounts with administrative privileges. Consider the same precautions for power users who have broad access to company data.
- Update and patch promptly to remove the risk of becoming a victim due to a previously known vulnerability.
- Conduct impromptu cybersecurity awareness training for all employees that reminds them not to open attachments or click unknown or untrusted links. This will help keep things front of mind for all employees.